रजिस्ट्री सं० डी० एल०-33004/99 REGD. NO. D. L.-33004/99

सत्यमेव जयते

भारत का राजपत्र
The Gazette of India

असाधारण

EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)

PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं. 203] नई दिल्ली, बुधवार, अप्रैल 13, 2011/चैत्र 23, 1933

No. 203] NEW DELHI, WEDNESDAY, APRIL 13, 2011/CHAITRA 23, 1933

संचार और सूचना प्रौद्योगिकी मंत्रालय

(प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 11 अप्रैल, 2011

सा.का.नि. 313(अ).— केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम 2000 (2000 का 21) की धारा 43क के साथ पठित धारा 87 की उपधारा (2) के खंड (णख) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, निम्नलिखित नियम बनाती है, अर्थात् :--

1. **संक्षिप्त नाम और प्रारंभ**- (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (युक्तियुक्त सुरक्षा व्यवहार और प्रक्रियाएं तथा संवेदनशील व्यक्तिगत डाटा या सूचना) नियम, 2011 है।

(2) ये राजपत्र में इनके प्रकाशन की तारीख से प्रवृत्त होंगे।

2. **परिभाषाएं**-(1) इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,-

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "जैवमिती" से ऐसी प्रौद्योगिकी अभिप्रेत है जो अधिप्रमाणन के प्रयोजनों के लिए "उंगलियों के निशान", "आँख का रेटिना और पुतली", "ध्वनि के पैटर्न", "मुख के पैटर्न", "हाथ का मापमान" और "डीएनए", जैसी मानव शरीर की विशिष्टियों का माप लेती हैं और विश्लेषण करती हैं;

(ग) "निगमित निकाय" से अधिनियम की धारा 43क के स्पष्टीकरण के खंड (i) में यथा परिभाषित निगमित निकाय अभिप्रेत है;

1330 GI/11—1A

(घ) "साइबर घटनाओं" से साइबर सुरक्षा के संबंध में कोई वास्तविक या आशंकित प्रतिकूल घटना अभिप्रेत है जो स्पष्ट रूप से या अस्पष्ट रूप से किसी लागू सुरक्षा नीति का अतिक्रमण करती है, जिसके परिणाम कोई अप्राधिकृत एक्सेस, सेवा का न मिलना या सेवा में बाधा, सूचना के प्रसंस्करण या भंडारण या डाटा, सूचना मे बिना प्राधिकार के परिवर्तन के लिए किसी कंप्यूटर संसाधन का अप्राधिकृत उपयोग कारित हुआ है;

(ङ) "डाटा" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ण) में यथा परिभाषित डाटा अभिप्रेत है;

(च) "सूचना" से अधिनियम की धारा 2 की उपधारा (1) के खंड (फ) में यथा परिभाषित सूचना अभिप्रेत है;

(छ) "मध्यवर्ती" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ब) में यथा परिभाषित मध्यवर्ती अभिप्रेत है;

(ज) "पासवर्ड" से ऐसा कोई गुप्त शब्द या पद या कूट या पास पद या गुप्त कुंजी, या एनक्रिप्शन या डिक्रिप्शन कुंजियां अभिप्रेत है जिनका उपयोग किसी व्यक्ति द्वारा किसी सूचना तक प्रवेश या एक्सेस बनाने के लिए किया जाता है;

(झ) "व्यक्तिगत सूचना" से ऐसी कोई सूचना अभिप्रेत है, जो किसी प्रकृत व्यक्ति से संबंधित है जो या तो प्रत्यक्ष रूप से अथवा अप्रत्यक्ष रूप से किसी अन्य उपलब्ध सूचना या ऐसी सूचना के, जिसके किसी निगमित निकाय को उपलब्ध होने की संभावना हो, साथ संयोजन में ऐसे व्यक्ति की पहचान करने में समर्थ हो।

(2) अन्य सभी प्रयुक्त शब्दों और पदों का, जो इन नियमों में परिभाषित नहीं है किंतु अधिनियम में परिभाषित हैं, क्रमशः वही अर्थ होगा जो अधिनियम में उनका है।

3. संवेदनशील व्यक्तिगत डाटा या सूचना.-- किसी व्यक्ति के संवेदनशील व्यक्तिगत डाटा या सूचना से ऐसी व्यक्तिगत सूचना अभिप्रेत है, जिसमें निम्नलिखित से संबंधित सूचना अंतर्विष्ट है, --

(i) पासवर्ड;

(ii) वित्तीय सूचना जैसे कि बैंक खाता या क्रेडिट कार्ड या डेबिट कार्ड या अन्य संदाय लिखत के ब्यौरे;

(iii) भौतिक, शरीर विज्ञान और मानसिक स्वास्थ्य की स्थिति;

(iv) लैंगिक रुझान;

(v) चिकित्सकीय अभिलेख और इतिहास;

(vi) जैवमिती सूचना;

(vii) उपरोक्त खंडों के संबंध में ऐसे कोई ब्यौरे, जो सेवा उपलब्ध कराने के लिए किसी निगमित निकाय को उपलब्ध कराए जाते हैं; और

(viii) निगमित निकाय द्वारा किसी विधिपूर्ण संविदा के अधीन या अन्यथा कार्यवाही, भंडारण या प्रसंस्करण के लिए उपरोक्त खंडों के अधीन प्राप्त कोई सूचना:

परंतु ऐसी कोई सूचना, जो आसानी से उपलब्ध है या लोक क्षेत्र में पहुंच के अधीन है या जिसे सूचना का अधिकार अधिनियम, 2005 या तत्समय प्रवृत्त किसी अन्य विधि के अधीन प्रस्तुत किया गया है, को इन नियमों के प्रयोजनों के लिए संवेदनशील व्यक्तिगत डाटा या सूचना नहीं समझा जाएगा।

4. *निगमित निकाय द्वारा सूचना की गोपनीयता और प्रकटन के लिए नीति का उपबंध किया जाना.*-- (1) निगमित निकाय या ऐसा कोई व्यक्ति जो निगमित निकाय की ओर से सूचना उपलब्ध कराने वाले व्यक्ति की सूचना को एकत्र करता, प्राप्त करता है, उसे कब्जे में रखता है, उसका भंडारण करता है, उस पर कार्यवाही या रखरखाव करता है, व्यक्तिगत सूचना, जिसके अंतर्गत संवेदनशील व्यक्तिगत डाटा या सूचना भी है, के रखरखाव या उस पर कार्यवाही करने के लिए एक गोपनीय नीति का उपबंध करेगा और यह सुनिश्चित करेगा कि वह सूचना ऐसी सूचना उपलब्ध करने वाले व्यक्तियों द्वारा, जिन्होंने किसी विधिपूर्ण संविदा के अधीन ऐसी सूचना उपलब्ध कराई है, देखने के लिए उपलब्ध है। ऐसी नीति को निगमित निकाय या उसकी ओर से किसी व्यक्ति द्वारा निगमित निकाय की वेबसाइट पर प्रकाशित किया जाएगा और उसमें निम्नलिखित के लिए उपबंध होगा--

(i) उसके व्यवहारों और नीतियों का स्पष्ट और आसानी से एक्सेस हो सकने वाला कथन;

(ii) नियम 3 के अधीन एकत्रित व्यक्तिगत या संवेदनशील व्यक्तिगत डाटा या सूचना की किस्म;

(iii) संग्रहण का प्रयोजन और ऐसी सूचना का उपयोग;

(iv) नियम 6 में यथा उपबंधित संवेदनशील वैयक्तिक डाटा या सूचना सहित सूचना का प्रकटन;

(v) नियम 8 के अधीन यथा उपबंधित युक्तियुक्त सुरक्षा पद्धतियां और प्रक्रियाएँ।

5. **सूचना का संग्रहण** - (1) निगमित निकाय या इसके निमित्त कोई अन्य व्यक्ति ऐसी सूचना के संग्रहण से पूर्व उपयोग के प्रयोजन के संबंध में संवेदनशील वैयक्तिक डाटा या सूचना प्रदाता से पत्र या फैक्स या ई-मेल के माध्यम से लिखित में सहमति प्राप्त करेगा।

(2) निगमित निकाय या इसके निमित्त कोई अन्य व्यक्ति संवेदनशील वैयक्तिक डाटा या सूचना संग्रहीत नहीं करेगा यदि -

(क) सूचना निगमित निकाय या इसके निमित्त किसी अन्य व्यक्ति के कृत्य या गतिविधि से संबंधित विधिपूर्ण प्रयोजन के लिए संग्रहीत नहीं की जा रही है; और

(ख) संवेदनशील वैयक्तिक डाटा या सूचना का संग्रहण उस प्रयोजन के लिए आवश्यक नहीं समझा जाता है ।

(3) संबंधित व्यक्ति से सीधे सूचना संग्रहण करते समय, निगमित निकाय या इसके निमित्त कोई अन्य व्यक्ति ऐसे कदम उठाएगा जो उन परिस्थितियों में निम्नलिखित सुनिश्चित करने के लिए युक्तियुक्त हों-

(क) संबंधित व्यक्ति को इस तथ्य की जानकारी है कि सूचना संग्रहीत की जा रही है;

(ख) संबंधित व्यक्ति को उस प्रयोजन की जानकारी है जिसके लिए सूचना संग्रहीत की जा रही है;

(ग) संबंधित व्यक्ति को सूचना के आशयित प्राप्तकर्ता की जानकारी है; और

(घ) संबंधित व्यक्ति को-

(i) उस अभिकरण के नाम और पते की ज़ानकारी है जो सूचना का संग्रहण कर रहा है; और

(ii) उस अभिकरण के नाम और पते की जानकारी है जो सूचना प्रतिधारित करेगा।

(4) संवेदनशील वैयक्तिक डाटा या सूचना रखने वाला निगमित निकाय या इसके निमित्त कोई अन्य व्यक्ति सूचना को उस प्रयोजन, जिसके लिए सूचना विधिपूर्वक प्रयोग की जा सकेगी या तत्समय प्रवृत्त किसी अन्य विधि के अधीन अन्यथा अपेक्षित, से अधिक समय तक प्रतिधारित नहीं करेगा।

(5) संग्रहीत सूचना उस प्रयोजन के लिए प्रयोग की जाएगी जिसके लि यह संग्रहीत की गई है।

(6) निगमित निकाय या इसके निमित्त कोई अन्य व्यक्ति सूचना ों को, जब उनके द्वारा अनुरोध किया जाए, उस सूचना के पुनर्विलोकन की अनुज्ञा देगा जो प्रदान की थी और सुनिश्चित करेगा कि कोई वैयक्तिक सूचना या संवेदनशील वैयक्तिक डाटा या सूचना गलत या अपर्याप्त पाए जाने पर यथासाध्य ठीक या संशोधित की जाएगी :

परंतु यह कि निगमित निकाय व्यक्तिगत सूचना या संवेदनशील डाटा या सूचना प्रदाता द्वार ऐसे निगमित निकाय या निगमित निकाय की ओर से कार्य करने वाले किसी अन्य व्यक्ति द्वारा आपूर्ति की गई सूचना की प्रामाणिकता के लिए उत्तरदायी नहीं होगा।

(7) निगमित निकाय या, उसकी ओर से कोई व्यक्ति संवेदनशील वैयक्तिक डाटा या सूचना, जिसके अंतर्गत संवेदनशील वैयक्तिक डाटा या सूचना भी है, के एकत्र करने से पूर्व सूचना प्रदाता को यह विकल्प प्रदान करेगा कि वह एकत्र किए जाने वाले वांछित डाटा या सूचना प्रदान न करें। सूचना प्रदाता को किसी भी समय सेवाओं का लाभ लेते समय या अन्यथा निगमित निकाय को पूर्व में दी गई अपनी सहमति वापस लेने का भी विकल्प होगा। सहमति का ऐसा वापस लिया जाना निगमित निकाय को लिखित में भेज दिया जाएगा। प्रदान करने वाले सूचना प्रदाता या बाद में अपनी सहमति वापस लेने की दशा में, निगमित निकाय को ऐसे माल या सेवाएँ प्रदान न करने का विकल्प होगा जिनके लिए उक्त सूचना मांगी गई थी।

(8) निगमित निकाय या उसकी ओर से कोई व्यक्ति नियम 8 में यथा उपबंधित अनुसार सूचना को सुरक्षित रखेगा।

(9) निगमित निकाय समयबद्ध रीति में सूचना के प्रसंस्करण के संबंध में अपने सूचना प्रदाता की किन्हीं विसंगतियों और शिकायतों का समाधान करेगा। इस प्रयोजन के लिए, निगमित निकाय

एक शिकायत अधिकारी पदाभिहित करेगा और अपनी वेबसाइट पर उसका नाम तथा संपर्क ब्यौरे प्रकाशित करेगा । शिकायत अधिकारी समीचीनतापूर्वक परन्तु सूचना प्राप्त किए जाने की तारीख से एक मास के भीतर सूचना प्रदाता की शिकायतों का समाधान करेगा।

6 **सूचना का प्रकटन** - (1) निगमित निकाय द्वारा किसी तीसरे पक्षकार को संवेदनशील वैयक्तिक डाटा या सूचना के प्रकटन के लिए उस प्रदाता से पूर्व अनुज्ञा अपेक्षित है जिसने विधिपूर्ण संविदा या अन्यथा ऐसी सूचना दी है सिवाए तब के जब निगमित निकाय और सूचना प्रदाता के बीच ऐसे प्रकटन पर किसी संविदा में सहमति हुई हो या जहाँ प्रकटन किसी विधिक बाध्यता का अनुपालन करने के लिए आवश्यक है।

परन्तु सूचना सूचना प्रदाता से पूर्व सहमति अभिप्राप्त किए बिना, पहचान के सत्यापन के पयोजन के लिए, या निवारण, पता लगाने, अन्वेषण जिसमें साइबर घटनाएँ भी हैं, अभियोजन और अपराधों के दण्ड के लिए संवेदनशील वैयक्तिक डाटा या सूचना सहित सूचना अभिप्राप्त करने के लिए विधि के अधीन आज्ञापित सरकारी अभिकरणों के साथ बांटी जाएगी। सरकारी अभिकरण ऐसी सूचना की मांग करने के प्रयोजन का स्पष्टत: उल्लेख करते हुए संवेदनशील वैयक्तिक डाटा या सूचना रखने वाले निगमित निकाय को लिखित में अनुरोध भेजेगा। सरकारी अभिकरण यह भी कथन करेगा कि इस प्रकार अभिप्राप्त सूचना प्रकाशित नहीं की जाएगी या किसी अन्य व्यक्ति को नहीं बताई जाएगी।

(2) उप नियम (1) में अन्तर्विष्ट किसी बात के होते हुए, कोई संवेदनशील डाटा या सूचना तत्समय प्रवृत्त विधि के अधीन किसी आदेश द्वारा किसी तृतीय पक्षकार को नहीं बताई जाएगी।

(3) निगमित निकाय या उसकी ओर से कोई व्यक्ति संवेदनशील वैयक्तिक डाटा या सूचना को प्रकाशित नहीं करेंगे।

(4) उप नियम (1) के अधीन निगमित निकाय या उसकी ओर से किसी व्यक्ति से संवेदनशील वैयक्तिक आंकड़े या सूचना को प्राप्त कारने वाला तृतीय पक्षकार उसका आगे प्रकटन नहीं करेगा।

(7) **सूचना का अंतरण** - कोई निगमित निकाय या उसकी ओर से कोई व्यक्ति भारत में या किसी अन्य देश में अवस्थित किसी अन्य निगमित निकाय या किसी व्यक्ति को किसी सूचना सहित संवेदनशील वैयक्तिक डाटा या सूचना का अन्तरण कर सकेगा जो ऐसे डाटा संरक्षण के स्तर को सुनिश्चित करता है जिसका इन नियमों के अधीन उपबंधित किए गए अनुसार निगमित निकाय द्वारा पालन किया जाता है; यह अंतरण केवल तभी अनुज्ञात किया जाएगा जब वह निगमित निकाय या उसकी ओर से किसी व्यक्ति और सूचना प्रदाता या जहां ऐसे व्यक्ति ने डाटा अन्तरण के लिए सहमति दे दी है, के बीच विधिपूर्ण संविदा के निष्पादन के लिए आदश्यक हो।

8. **युक्तियुक्त सुरक्षा पद्धतियां और प्रक्रियाँ** - (1) कोई निगमित निकाय या उसकी ओर से किसी व्यक्ति पर, उनके द्वारा युक्तियुक्त सुरक्षा पद्धतियों और प्रक्रियाओं का अनुपालन कर लिए जाने के पश्चात ही विचार

किया जाएगा· यदि उन्होंने ऐसी सुरक्षा पद्धतियों और मानकों को कार्यान्वित कर दिया है और उनके पास ऐसा व्यापक प्रलेखित सूचना सुरक्षा कार्यक्रम और सूचना सुरक्षा नीतियां हैं जिनमें ऐसे प्रबंधकीय, तकनीकी, संक्रेथात्मक और भौतिक सुरक्षा नियंत्रण उपाय है जो कारबार की प्रकृति के साथ संरक्षित की जा रही सूचना आस्तियों के अनुरूप हैं। सूचना सुरक्षा भंग की दशा में, निगमित निकाय या उसकी ओर से किसी व्यक्ति से, जब कभी विधि के अधीन आज्ञापित अभिकरण द्वारा ऐसा करने की अपेक्षा की जाए, कि उन्होंने अपने प्रलेखित सूचना सुरक्षा कार्यक्रम और सूचना सुरक्षा नीतियों के अनुसार सुरक्षा नियंत्रण उपायों को कार्यान्वित किया है प्रदर्शित करने की अपेक्षा होगी।

(2) "सूचना प्रौद्योगिकी पर. आईएस/आईएसओ/आईईसी 27001 अंतर्राष्ट्रीय मानक सूचना तकनीकें-सूचना सुरक्षा प्रबध प्रणाली-अपेक्षाएँ" एक ऐसा मानक है जो उप नियम (1) में निर्दिष्ट है।

(3) किसी ऐसे संगम द्वारा बनाए गए किसी उद्योग संगम या अस्तित्व, जिसके सदस्य उप नियम (2) के अनुसार डाटा संरक्षण संबंधी उत्तम पद्धतियों के आईएस/आईएसओ/आईईसी कूट से भिन्न का अनुसरण करते स्व-विनियमनकारी हैं, अपनी उत्तम पद्धतियों के कूटों के प्रभावी कार्यान्वयन के लिए केन्द्रीय सरकार द्वारा सम्यकत: अनुमोदित और अधिसूचित सर्वोत्तम पद्धति कूट प्राप्त करेंगे।

(4) निगमित निकाय या उसकी ओर से कोई व्यक्ति, जिसने उप नियम (3) के अधीन यथा अनुमोदित और अधिसूचित या तो आईएस/आईएसओ/आईईसी27001 मानक को या डाटा संरक्षण संबंधी उत्तम पद्धतियों के कूटों को कार्यान्वित किया है, द्वारा युक्तियुक्त सुरक्षा पद्धतियों और प्रक्रियाओं का अनुपालन किया गटा समझा जाएगा परन्तु ऐसा मानक या उत्तम पद्धतियों के कूटों को केन्द्रीय सरकार द्वारा सम्यकत: अनुमोदित स्वतंत्र लेखा परीक्षक के माध्यम से अस्तित्वों द्वारा निगमित आधार पर प्रमाणित या संपरीक्षित करा लिया गया हो। युक्तियुक्त सुरक्षा पद्धतियों और प्रक्रियाओं की संपरीक्षा वर्ष में कम से कम एक बार की जाएगी या जब कभी निगमित निकाय या उसकी ओर से कोई व्यक्ति उसकी प्रक्रिया और कम्प्यूटर संसाधन के उल्लेखनीय उन्नयन आरंभ करता है ।

[फा. सं. 11(3)/2011-सीएलएफई]

एन. रवि शंकर, संयुक्त सचिव

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)
NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 313(E).— In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. **Short title and commencement.**— (1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette

2. **Definitions.** — (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

(c) "Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;

~~(d)~~ "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(h) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

(i) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

4. Body corporate to provide policy for privacy and disclosure of information.— (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal data or information collected under rule 3;

(iii) purpose of collection and usage of such information;

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8.

5. Collection of information.— (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

(a) the fact that the information is being collected;

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and

(d) the name and address of —

(i) the agency that is collecting the information; and

(ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force..

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf shall permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by

the provider of information to such body corporate or any other person acting on behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances of provider of information expeditiously but within one month from the date of receipt of grievance.

6. Disclosure of information.— (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contained in sub-rule (1), any sensitive personal data or Information shall be disclosed to any third party by an order under the law for the time being in force.

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

8. Reasonable Security Practices and Procedures.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities

through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

[F. No. 11(3)/2011-CLFE]
N. RAVI SHANKER, Jt. Secy.

अधिसूचना

नई दिल्ली, 11 अप्रैल, 2011

सा.का.नि. 314(अ).—केंद्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 79 की उप-धारा (2) के साथ पठित धारा 87 की उप-धारा (2) के खंड (यछ) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात :-

1. **संक्षिप्त नाम और प्रारंभ** – (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्यो[illegible]र्तियों के लिए दिशानिर्देश) नियम 2011 है।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे।

2. **परिभाषाएं** – (1) इन नियमों में जब तक कि संदर्भ से अन्यथा अपेक्षित न हो, -

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "संचार लिंक" से हाइपरटेक्सट या ग्राफिकल एलीमेंट (बटन, ड्राइंग, इमेज) के बीच संबंध अभिप्रेत है और समान या भिन्न इलेक्ट्रॉनिक दस्तावेज में एक या अधिक ऐसी मदें हैं जिनमें हाइपरलिंक्ड मद पर क्लिक करने पर उपयोक्ता को स्वत: हाइपरलिंक के दूसरे छोर पर अंतरित कर दिया जाता है जो कि कोई अन्य दस्तावेज या अन्य वेबसाइट या ग्राफिकल एलीमेंट हो सकता है;

(ग) "कम्प्यूटर संसाधन" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (ट) में यथा परिभाषित कम्प्यूटर संसाधन अभिप्रेत है;

(घ) "साइबर सुरक्षा घटना" से किसी साइबर सुरक्षा के संबंध में कोई वास्तविक या संदेहस्पद प्रतिकूल घटना अभिप्रेत है जो स्पष्ट रूप से या अस्पष्ट रूप से सुरक्षा नीति का अतिक्रमण करती है जिसका परिणाम कोई अप्राधिकृत एक्सेस, सेवा का न मिलना या सेवा में बाधा, सूचना के प्रसंस्करण या भंडारण या डाटा में बिना प्राधिकार के परिवर्तन के लिए किसी कम्प्यूटर संसाधन का अप्राधिकृत उपयोग कारित हुआ है;

(ङ) "डाटा" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (ण) में यथा परिभाषित डाटा अभिप्रेत है;

(च) "इलेक्ट्रॉनिक हस्ताक्षर" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (मक) में यथा परिभाषित इलेक्ट्रॉनिक हस्ताक्षर अभिप्रेत है;

(छ) "भारतीय कम्प्यूटर आपातस्थिति प्रत्युत्तर दल" से अधिनियम की धारा 70-ख की उप-धारा (1) के अधीन नियुक्त भारतीय कम्प्यूटर आपातस्थिति प्रत्युत्तर दल अभिप्रेत है;

(ज) "सूचना" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (फ) में यथा परिभाषित सूचना अभिप्रेत है;

(झ) "मध्यवर्ती" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (ब) में यथा परिभाषित मध्यवर्ती अभिप्रेत है;

(ञ) "उपयोक्ता" से कोई व्यक्ति अभिप्रेत है जो मध्यवर्ती के किसी कम्प्यूटर साधन का प्रयोग सूचन को होस्ट करने, प्रकाशित करने, बाँटने, संव्यवहार करने, प्रदर्शित करने या अपलोड करने या देखने के लिए करता है या उन्हें एक्सेस करता है और इसमें अन्य व्यक्ति भी हैं जो संयुक्त रूप से किसी साइबर कैफे में कम्प्यूटर संसाधनों का उपयोग करते हैं या एक्सेस करते हैं।

(2) अन्य सभी प्रयुक्त शब्दों और पदों का जो इन नियमों में परिभाषित नहीं है किन्तु अधिनियम में परिभाषित है, क्रमशः वही अर्थ होगा जो अधिनियम में उनका है।

3. **मध्यवर्ती द्वारा अनुपालन के लिए सम्यक् कर्मिष्ठता** - मध्यवर्ती अपने कर्तव्यों का निर्वहन करते हुए निम्नलिखित सम्यक् कर्मिष्ठता का अनुपालन करेगा, अर्थात :-

(1) मध्यवर्ती किसी व्यक्ति द्वारा मध्यवर्ती के कम्प्यूटर संसाधनों के एक्सेस या प्रयोग के लिए नियमों और विनियमों, एकांतता नीति और उपयोक्ता करार का प्रकाशन करेगा।

(2) ऐसे नियम और विनियम, निबंधन और शर्तें या उपयोक्ता करार कम्प्यूटर संसाधनों के उपयोक्ताओं को सूचित करेंगे कि वह ऐसी किसी सूचना को होस्ट, प्रदर्शित, अपलोड, उपांतरित, प्रकाशित, पारेषण, अपडेट या बांटे नहीं जो कि -

(क) किसी और व्यक्ति से संबंध रखती है और जिस पर उपयोक्ता का कोई अधिकार नहीं है;

(ख) समग्र रूप से हानिकारक, उत्पीड़क, ईशनिंदक, मानहानिकारक, अश्लील, पोर्नोग्राफिक, पेडोफिलिया, अपलेखात्मक, अन्य व्यक्ति की एकांतता के लिए आक्रामक, घृणास्पद, या प्रजाती, जातीय रूप से आक्षेप योग्य, अवमनित अपमानजनक, धनशोधन या द्यूत से संबंधित या उसे बढ़ावा देने के लिए या अन्यथा चाहे जो हो किसी अन्य रीति में विधिविरुद्ध है;

(ग) किसी भी प्रकार से अवयस्कों के लिए हानिकरक है;

(घ) किसी पेटेंट, व्यापार चिह्न, प्रतिलिप्याधिकार या अन्य सांपत्तिक अधिकारों का उल्लंघन करता है;

(ङ) तत्समय प्रवृत किसी विधि का अतिक्रमण करता है;

(च) ऐसे संदेश के मूल के विषय में प्रेषिती को धोखा देता है या बहकाता है या ऐसी सूचना का संचार करता है जो समग्र रूप से घृणास्पद या धमकाने वाली प्रकृति की है;

(छ) किसी अन्य व्यक्ति का प्रतिरूपण करता है;

(ज) ऐसे सॉफ्टवेयर वायरस या अन्य कम्प्यूटर कूट, फाइल या प्रोग्राम अंतर्विष्ट हैं जो किसी कम्प्यूटर संसाधन की कार्यशीलता को बाधित करने, नष्ट करने या संशोधित करने के लिए डिजाइन किए गए हैं;

(झ) भारत की एकता, अखंडता, रक्षा, सुरक्षा या प्रभुता, विदेशी राज्यों से मित्रता के संबंधों या लोक व्यवस्था को खतरे में डालता है या किसी संज्ञेय अपराध को कारित करने के लिए उकसाता है या किसी अन्य राष्ट्र का अपमान करता है ।

(3) मध्यवर्ती जानबूझकर ऐसी सूचना को होस्ट या प्रकाशित नहीं करेगा या उसके पारेषण को आरम्भ नहीं करेगा, उसके प्राप्तकर्ता का चयन नहीं करेगा और उपनियम (2) में यथा विनिर्दिष्ट पारेषण में अंतर्विष्ट सूचना का चयन या उपांतरण नहीं करेगा:

परन्तु यह कि मध्यवर्ती के निम्नलिखित कृत्य उपनियम (2) में यथाविर्निदिष्ट अनुसार ऐसी सूचना को होस्ट करना, प्रकाशित करना, संपादित करना या भंडारण करना नहीं माने जाएंगे -

(क) किसी कम्प्यूटर संसाधान में स्वतः किसी सूचना का अस्थायी या अल्पकालिक या मध्यवर्ती भंडारण उस कम्प्यूटर प्रणाली के अन्तर्भूत लक्षण के रूप में जिसमें अग्रेषित पारेषण या अन्य कम्प्यूटर संसाधन को संचार के लिए मानव संपादन नियंत्रण का निर्वहन अंतर्वलित नहीं है;

(ख) किसी मध्यवर्ती द्वारा किसी सूचना, डाटा या संचार संपर्क के एक्सेस को ऐसी सूचना, डाटा या संचार संपर्क के मध्यवर्ती द्वारा प्राधिकृत व्यक्ति की वास्तविक जानकारी में आने के पश्चात अधिनियम के उपबंधों के अनुसार किसी आदेश या निदेश के अनुसरण में हटाना ;

(4) मध्यवर्ती, जिसकी कम्प्यूटर प्रणाली पर सूचना भंडारित या होस्ट या प्रकाशित की गई है, स्वयं जानकारी अभिप्राप्त करने पर या किसी प्रभावित व्यक्ति द्वारा लिखित में या इलेक्ट्रॉनिक हस्ताक्षर से हस्ताक्षरित ई-मेल द्वारा पूर्वोक्त उपनियम (2) में यथावर्णित सूचना वास्तविक जानकारी में लाए जाने पर 36 घंटे के भीतर कार्रवाई करेगा और जहां लागू हो ऐसी सूचना के उपयोक्ता या स्वामी के साथ ऐसी सूचना को निष्क्रिय करने का कार्य करेगा जो कि उपनियम (2) का उल्लंघन करती है। इसके अलावा मध्यवर्ती ऐसी सूचना और सहबद्ध अभिलेखों को अन्वेषण के प्रयोजनों के लिए कम से कम 90 दिन की अवधि के लिए परिरक्षित रखेगा।

(5) मध्यवर्ती उपयोक्ताओं को सूचित करेगा कि मध्यवर्ती के कम्प्यूटर संसाधनों का एक्सेस या उपयोग करने के लिए नियमों और विनियमों, उपयोक्ता करार, एंकातता नीति का अननुपालन करने पर मध्यवर्ती को मध्यवर्ती के कम्प्यूटर संसाधनों को एक्सेस करने या उपयोग करने के उपयोक्ताओं के अधिकार को समाप्त करने का और अननुपालन की गई सूचना को हटाने का अधिकार होगा।

(6) मध्यवर्ती अधिनियम के उपबंधों का या तत्समय प्रवृत अन्य विधियों का सख्ती से अनुपालन करेगा।

(7) मध्यवर्ती विधिपूर्वक प्राधिकृत सरकारी अभिकरणों को साइबर सुरक्षा गतिविधि का अन्वेषण, संरक्षण करने के लिए सूचना या ऐसी सहायता उपलब्ध कराएगा जो विधिपूर्ण आदेश द्वारा अपेक्षित हो

सूचना या ऐसी सहायता पहचान के सत्यापन के प्रयोजनों के लिए या निवारण, पता लगाने, अन्वेषण, अभियोजन, साइबर सुरक्षा की घटना और तत्समय प्रवृत किसी विधि के अधीन अपराधों के लिए दंड के लिए लिखित में अनुरोध पर जिसमें ऐसी सूचना या ऐसी सहायता की वांछा का प्रयोजन स्पष्ट रूप से दर्शाया गया हो, के प्रयोजन के लिए उपलब्ध करायी जाएगी।

(8) मध्यवर्ती सूचना प्रौद्योगिकी (युक्तियुक्त सुरक्षा पद्धतियां और प्रक्रिया तथा संवेदनशील वैयक्तिक सूचना) नियम 2011 में यथा विहित युक्तियुक्त सुरक्षा पद्धतियों और प्रक्रियाओं का अनुसरण करके अपने कम्प्यूटर संसाधनों और उनमें अंतर्विष्ट सूचना की सुरक्षा के लिए युक्तियुक्त उपाय करेगा।

(9) मध्यवर्ती साइबर सुरक्षा की घटनाएँ और साइबर सुरक्षा की घटनाओं से संबंधित सूचना को भारतीय कम्प्यूटर आपातास्थिति प्रत्युतर दल के साथ बांटेगा।

(10) मध्यवर्ती जानबूझकर कम्प्यूटर संसाधनों की तकनीकी आकृति को स्थापित या प्रतिष्ठापित या उपांतरित नहीं करेगा या ऐसे किसी कृत्य में भागीदार नहीं बनेगा जिससे कम्प्यूटर संसाधन के सामान्य कृत्य उससे भिन्न होने की संभावना हो जो कि उसके द्वारा निष्पादित किया जाना आशयित है जिससे तत्समय प्रवृत किसी विधि की परवंचना हो:

परन्तु यह कि मध्यवर्ती कम्प्यूटर संसाधन और उसमें अंतर्विष्ट सूचना की सुरक्षा के एकमात्र उद्देश्य के लिए प्रौद्योगिकीय साधनों, का विकास कर सकता है, उत्पादन कर सकता है, वितरण कर सकता है या उन्हें नियंत्रित कर सकता है।

(11) मध्यवर्ती अपनी बेवसाइट पर शिकायत अधिकारी का नाम और उसके संपर्क ब्यौरे के साथ-साथ उस प्रक्रिया को भी प्रकाशित करेगा जिसके द्वारा कोई उपयोक्ता या अन्य पीड़ित जो नियम 3 के अतिक्रमण में किसी व्यक्ति द्वारा कम्प्यूटर संसाधन के एक्सेस या उपयोग के कारण उसके द्वारा उपलब्ध कराए गए कम्प्यूटर संसाधनों से संबंधित अन्य मामले के कारण पीड़ित हुआ है, ऐसे एक्सेस या मध्यवर्ती कम्प्यूटर सासंधनों के उपयोग के विरुद्ध अपनी शिकायतों को नोट करा सके। शिकायत अधिकारी शिकायतों का प्रतितोष शिकायत मिलने की तारीख से एक मास की अवधि के भीतर करेगा ।

[फा. सं. 11(3)/2011-सीएलएफई]

एन. रवि शंकर, संयुक्त सचिव

NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 314(E).— In exercise of the powers conferred by clause (zg) of sub-section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: —

1. **Short title and commencement**.— (1) These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions**.— (1) In these rules, unless the context otherwise requires,—

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Communication link" means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element.

(c) "Computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(d) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

(g) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub section (1) of section 70(B) of the Act;

(h) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(i) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(j) "User" means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Due diligence to be observed by intermediary.— The intermediary shall observe following due diligence while discharging his duties, namely : —

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2):

provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule (2) —

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non-compliant information..

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for

investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force:

provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

[F. No. 11(3)/2011-CLFE]
N. RAVI SHANKER, Jt. Secy.

अधिसूचना

नई दिल्ली, 11 अप्रैल, 2011

सा.का.नि. 315(अ).— केंद्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 79 की उप-धारा (2) के साथ पठित धारा 87 की उप-धारा (2) के खंड (यछ) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात :-

1. संक्षिप्त नाम और प्रारंभ – (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (साइबर कैफे के लिए दिशानिर्देश) नियम 2011 है।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे।

2. परिभाषाएं – (1) इन नियमों में जब तक कि संदर्भ से अन्यथा अपेक्षित न हो, -

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "समुचित सरकार" से केंद्रीय सरकार या राज्य सरकार या संघ राज्य क्षेत्र का प्रशासन अभिप्रेत है;

(ग) "साइबर कैफे" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (ढक) में यथा परिभाषित साइबर कैफे अभिप्रेत है;

(घ) "कम्प्यूटर संसाधन" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (ट) में यथा परिभाषित कम्प्यूटर संसाधन अभिप्रेत है;

(ङ) "डाटा" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (फ) में यथा परिभाषित डाटा अभिप्रेत है;

(च) "सूचना" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (फ) में यथा परिभाषित सूचना अभिप्रेत है;

(छ) "मध्यवर्ती" से अधिनियम की धारा 2 की उप-धारा (1) के खंड (ब) में यथा परिभाषित मध्यवर्ती अभिप्रेत है;

(ज) "रजिस्ट्रीकरण अभिकरण" से समुचित सरकार द्वारा पदाविहित कोई अभिकरण अभिप्रेत है जो अपने प्रचालन के लिए साइबर कैफे को रजिस्ट्रीकृत करे;

(झ) "लॉग रजिस्टर" से साइबर कैफे द्वारा कम्प्यूटर संसाधनों के एक्सेस और अनुप्रयोग के लिए अनुरक्षित रजिस्टर अभिप्रेत है;

(ञ) "प्रयोक्ता" से कोई व्यक्ति अभिप्रेत है जो कम्प्यूटर साधनों का प्रयोग करता है या उन्हें एक्सेस करता है और इसमें अन्य व्यक्ति भी हैं जो संयुक्त रूप से किसी साइबर कैफे में कम्प्यूटर संसाधनों का उपयोग करते हैं या एक्सेस करते हैं।

(2) अन्य सभी प्रयुक्त शब्दों और पदों का जो इन नियमों में परिभाषित नहीं है किन्तु अधिनियम में परिभाषित हैं क्रमशः वही अर्थ होगा जो उन्हें अधिनियम में उनका है।

3. **साइबर कैफे का रजिस्ट्रीकरण करने के लिए अभिकरण** - (1) सभी साइबर कैफे को समुचित सरकार द्वारा यथा अधिसूचित रजिस्ट्रीकरण अभिकरण नामक अभिकरण द्वारा अनन्य रजिस्ट्रीकरण संख्या के साथ रजिस्टर किया जाएगा। रजिस्ट्रीकरण के मुख्य निबंधनों में शामिल हैं :

(i) प्रतिष्ठापन का नाम;
(ii) पता और संपर्क के ब्यौरे इसमें ई-मेल भी शामिल है;
(iii) क्या वैयक्तिक या भागीदारी या एकल स्वत्वधारी या संस्था या कंपनी है;
(iv) निगमन की तारीख;
(v) स्वामी/भागीदार/स्वत्वधारी/निदेशक का नाम;
(vi) क्या रजिस्ट्रीकृत है अथवा नहीं (यदि हां, तो फर्मों के रजिस्ट्रार के पास रजिस्ट्रीकरण की प्रति या कंपनी अथवा संस्था रजिस्ट्रार के पास रजिस्ट्रीकरण की प्रति); और
(vii) साइबर कैफे से प्रदान की जाने वाली सेवा का प्रकार।

साइबर कैफे के रजिस्ट्रीकरण के पश्चात रजिस्ट्रीकरण अभिकरण के किसी अधिकारी द्वारा वास्तविक निरीक्षण किया जाएगा।

(2) साइबर कैफे के रजिस्ट्रीकरण के ब्यौरे रजिस्ट्रीकरण अभिकरण की वेबसाइट पर प्रकाशित किए जाएंगे।

(3) समुचित सरकार साइबर कैफे को ऑन-लाइन रजिस्टर करने के लिए ऑन-लाइन रजिस्ट्रीकरण की सुविधा स्थापित करने का प्रयास करेगी।

(4) समुचित सरकार द्वारा अधिसूचित रजिस्ट्रीकरण अभिकरण द्वारा रजिस्ट्रीकरण की विस्तृत प्रक्रिया का अनुपालन करना अनिवार्य होगा जिसे केन्द्रीय सरकार द्वारा इन नियमों के अन्तर्गत अलग से अधिसूचित किया जाएगा।

4. **उपयोक्ताओं की पहचान** - (1) साइबर कैफे किसी प्रयोक्ता को अपने कम्प्यूटर संसाधनों के उपयोक्ता की पहचान स्थापित किए बिना उपयोग अनुज्ञात नहीं करेगा। उपयोग करने का आशय रखने वाला उपयोक्ता ऐसे दस्तावेज प्रस्तुत करके अपनी पहचान स्थापित करेगा जिससे साइबर कैफे के पास उपयोक्ता की पहचान समाधानप्रद रूप से हो सके। ऐसे दस्तावेजों में निम्नलिखित में से कोई हो सकेगा :-

(i) विद्यालय या महाविद्यालय द्वारा जारी पहचान पत्र; या
(ii) बैंक या डाकघर द्वारा जारी फोटो क्रेडिट कार्ड या डेबिट कार्ड; या

(iii) पासपोर्ट; या

(iv) मतदाता पहचान पत्र; या

(v) आयकर प्राधिकरण द्वारा जारी स्थायी लेखा संख्या; या

(vi) नियोक्ता या किसी सरकारी अभिकरण द्वारा जारी फोटो पहचान पत्र; या

(vii) समुचित सरकार द्वारा जारी चालन अनुज्ञप्ति; या

(viii) भारत अनन्य पहचान प्राधिकरण (यूआईडीआई) द्वारा जारी अनन्य पहचान संख्या (यूआईडी)।

(2) साइबर कैफे उपयोक्ता दस्तावेजों का अभिलेख उपयोक्ता द्वारा और साइबर कैफे के प्राधिकृत प्रतिनिधि द्वारा समयक्त: प्राधिकृत दस्तावेज की फोटो प्रति या स्कैंड प्रति को भंडारित करके रखेगा: ऐसे अभिलेख का कम से कम एक वर्ष की अवधि के लिए अनुरक्षण किया जाएगा।

(3) उप-नियम (1) के अधीन किसी उपयोक्ता द्वारा स्थापित पहचान के अतिरिक्त, उसका साइबर कैफे में उपयोक्ता को पहचान स्थापित करने के लिए किसी एक कम्प्यूटर पर प्रतिष्ठापित वेब कैमरे का प्रयोग करके फोटो लिया जा सकेगा। उपयोक्ता और साइबर कैफे के प्राधिकृत प्रतिनिधि द्वारा समयक्त. प्राधिकृत ऐसे वेब कैमरे के फोटो लॉग रजिस्टर का भाग होंगे जिसे भौतिक या इलेक्ट्रॉनिक स्वरूप में अनुरक्षित रखा जा सकेगा।

(4) फोटो पहचान कार्ड के बिना किसी अवयस्क के साथ कोई वयस्क उप-नियम (1) के अधीन अपेक्षित किसी भी दस्तावेज के साथ होगा।

(5) किसी उपयोक्ता के साथ किसी व्यक्ति का साइबर कैफे में प्रवेश तब अनुज्ञात किया जाएगा जब उसने उप-नियम (1) मे सूचीबद्ध दस्तावेजों में से एक प्रस्तुत करके अपनी पहचान स्थापित कर दी हो और उसका अभिलेख उप-नियम (2) के अनुसार रखा जाएगा।

(6) साइबर कैफे संबंधित पुलिस को तुरंत रिपोर्ट करेगा यदि उन्हें किसी उपयोक्ता के संबंध में युक्तियुक्त संदेह या संशय हो।

5. **लॉग रजिस्टर** - (1) नियम 4 के उप-नियम (1) के अनुसार किसी उपयोक्ता और उसके साथ किसी अन्य व्यक्ति की पहचान स्थापित होने के पश्चात साइबर कैफे यथास्थिति प्रत्येक उपयोक्ता के साथ के व्यक्ति की अपेक्षित सूचना को लॉग रजिस्टर में न्यूनतम एक वर्ष की अवधि के लिए अभिलिखित करेगा और उसका अनुरक्षण करेगा।

(2) साइबर कैफे लॉग रजिस्टर के ऑन-लाइन संस्करण का अनुरक्षण कर सकेगा। लॉग रजिस्टर के ऐसे ऑन-लाइन संस्करण को डिजिटल या इलेक्ट्रॉनिकी हस्ताक्षर के माध्यम से प्राधिकृत किया जाएगा। लॉग रजिस्टर में प्रयोक्ता के कम से कम निम्नलिखित ब्यौरे अंतर्विष्ट होंगे, अर्थात :-

(i) नाम

(ii) पता

(iii) लिंग

(iv) संपर्क संख्या
(v) पहचान दस्तावेज की किस्म और ब्यौरा
(vi) तारीख
(vii) कंप्यूटर टर्मिनल की पहचान
(viii) लॉग-इन समय
(ix) लॉग-आउट समय

(3) साइबर कैफे लॉग-रजिस्टर की एक मासिक रिपोर्ट प्रस्तुत करेगा जिसमें कम्प्यूटर संसाधनों के उपयोग के तारीख-वार ब्यौरे उपदर्शित होंगे और इसकी एक हार्ड और साफ्ट प्रति रजिस्ट्रीकरण अभिकरण द्वारा यथानिदेशित व्यक्ति या अभिकरण को प्रत्येक मास की 5 तारीख तक प्रस्तुत करेगा।

(4) साइबर कैफे का स्वामी किसी उपयोक्ता द्वारा उसके कम्प्यूटर संसाधनों के प्रत्येक एक्सेस या लॉग-इन के निम्नलिखित लॉग अभिलेखों के बैकअप का भंडारण और अनुरक्षण कम से कम एक वर्ष के लिए करने का उत्तरदायी होगा :-

(i) साइबर कैफे में कम्प्यूटर संसाधनों का प्रयोग करके एक्सेस की गई वेबसाइटों का इतिहास;
(ii) साइबर कैफे में प्रतिष्ठापित प्रोक्सी सरवर के लॉग।

साइबर कैफे भारतीय कम्प्यूटर आपातस्थिति प्रत्युत्तर दल (सीईआरटी-इन) द्वारा तैयार और समय-समय पर अद्यतन "सीआईएसजी-2008-01 की ऑडिटिंग और लॉगिंग दिशानिर्देश" को लॉग से संबंधित किसी सहायता के लिए निर्दिष्ट कर सकेगा। यह दस्तावेज www.cert-in.org.in पर उपलब्ध है।

(5) साइबर कैफे यह सुनिश्चित करेगा कि लॉग रजिस्टर में परिवर्तन न किया जाए और उसका कम से कम एक वर्ष की अवधि के लिए सुरक्षित रीति में अनुरक्षण किया जाए।

6. **भौतिक विन्यास और कम्प्यूटर संसाधन का प्रबंधन** – (1) साइबर कैफे में निर्मित या प्रतिष्ठापित विभाजन या प्रकोष्ठ यदि कोई हों, फर्श के स्तर से साढ़े चार फुट से अधिक नहीं होंगे।

(2) विभाजनों या प्रकोष्ठों में प्रतिष्ठापित कम्प्यूटरों से भिन्न कम्प्यूटरों का स्क्रीन बाहर की तरफ होगा अर्थात वह साइबर कैफे में सामान्य खुले स्थान की ओर होंगे।

(3) कोई भी साइबर कैफे जिसमें प्रकोष्ठ या विभाजन है अवयस्कों को सिवाए तब कि जब वह अपने संरक्षकों या अभिभावकों के साथ हों किसी कम्प्यूटर संसाधन का प्रयोग करने के लिए अनुज्ञात नहीं करेगा।

(4) साइबर कैफे में प्रतिष्ठापित कम्प्यूटर प्रणालियों और सरवरों की सभी घड़ियों को भारतीय मानक समय के साथ समकालिक किया जाएगा।

(5) साइबर कैफे में सभी कम्प्यूटर वाणिज्यिक रूप से उपलब्ध सुरक्षा या फिल्टरिंग सॉफ्टवेयर से सुसज्जित हो सकेंगे ताकि जहां तक संभव हो अश्लील वेबसाइटों जिसमें बाल अश्लील या अश्लील सूचना की वेबसाइटों तक एक्सेस को रोका जा सके।

(6) साइबर कैफे यह सुनिश्चय करने के लिए पर्याप्त पूर्वोपाय करेगा कि उनके कम्प्यूटर संसाधन का उपयोग किसी अवैध गतिविधि के लिए न किया जाए।

(7) साइबर कैफे एक बोर्ड को प्रदर्शित करेगा जो प्रयोक्ताओं को स्पष्ट रूप से दृश्य हो कि अश्लील साइटों को देखने के साथ-साथ ऐसी सूचना को कापी करना या डाउनलोड करना प्रतिषिद्ध है जो विधि के अधीन प्रतिषिद्ध है।

(8) साइबर कैफे कम्प्यूटर प्रणाली की सेटिंग में फेरफार करने से प्रयोक्ताओं को अननुज्ञात करने के लिए युक्तियुक्त निवारक उपाय करेगा।

(9) साइबर कैफे उपयोक्ता पहचान सूचना और लॉग रजिस्टर का अनुरक्षण सुरक्षित रीति में करेगा।

(10) साइबर कैफे अपने कर्मचारीवृद्ध का अभिलेख भी एक वर्ष की अवधि के लिए अनुरक्षित रखेगा।

(11) साइबर कैफे लॉग रजिस्टर की सूचना का दुरूपयोग या उसमें परिवर्तन नहीं करेगा।

7. **साइबर कैफे का निरीक्षण** : रजिस्ट्रीकरण अभिकरण द्वारा प्राधिकृत कोई अधिकारी इन नियमों की अनुपालना में किसी भी समय साइबर कैफे और कम्प्यूटर संसाधनों या उसमे प्रतिष्ठापित नेटवर्क की जांच या निरीक्षण करने के लिए प्राधिकृत है। साइबर कैफे का स्वामी मांग करने पर निरीक्षण करने वाले अधिकारी को संबंधित दस्तावेज, रजिस्टर और अन्य अपेक्षित सूचना उपलब्ध कराएगा।

[फा. सं. 11(3)/2011-सीएलएफई]

एन. रवि शंकर, संयुक्त सचिव

NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 315(E).— In exercise of the powers conferred by clause (zg) of sub-section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:—

1. **Short title and commencement.**— (1) These rules may be called the Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions.**— (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);
(b) "Appropriate Government" means the Central Government or the State Government or an Union Territory Administration;
(c) "Cyber Cafe" means cyber café as defined in clause (na) of sub-section (1) of section 2 of the Act;
(d) "computer resource" means a computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;
(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;
(h) "Registration Agency" means an agency designated by the Appropriate Government to register cyber café for their operation;
(i) "Log Register" – means a register maintained by the Cyber Café for access and use of computer resource;

(j) "User" means a person who avails or access the computer resource and includes other persons jointly participating in availing or accessing the computer resource in a cyber café.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Agency for registration of cyber café.— (1) All cyber cafes shall be registered with a unique registration number with an agency called as registration agency as notified by the Appropriate Government in this regard. The broad terms of registration shall include:

(i) name of establishment;
(ii) address with contact details including email address;
(iii) whether individual or partnership or sole properitership or society or company;
(iv) date of incorporation;
(v) name of owner/partnet/properiter/director;
(vi) whether registered or not (if yes, copy of registration with Registrar of Firms or Registrar of Companies or Societies); and
(vii) type of service to be provided from cyber café

Registration of cyber café may be followed up with a physical visit by an officer from the registration agency.

(2) The details of registration of cyber café shall be published on the website of the registration agency.

(3) The Appropriate Government shall make an endeavour to set up on-line registration facility to enable cyber café to register on-line.

(4) The detailed process of registration to be mandatorily followed by each Registration Agency notified by the Appropriate Government shall be separately notified under these rules by the central Government.

4. Identification of User.— (1) The Cyber Café shall not allow any user to use its computer resource without the identity of the user being established. The intending user may establish his identify by producing a document which shall identify the users to the satisfaction of the Cyber Café. Such document may include any of the following :—

(i) Identity card issued by any School or College; or

(ii) Photo Credit Card or debit card issued by a Bank or Post Office; or

(iii) Passport; or

(iv) Voter Identity Card; or

(v) Permanent Account Number (PAN) card issued by Income-Tax Authority; or

(vi) Photo Identity Card issued by the employer or any Government Agency; or

(vi) Driving License issued by the Appropriate Government; or

(vii) Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

(2) The Cyber Café shall keep a record of the user identification document by either storing a photocopy or a scanned copy of the document duly authenticated by the user and authorised representative of cyber cafe. Such record shall be securely maintained for a period of at least one year.

(3) In addition to the identity established by an user under sub-rule (1), he may be photographed by the Cyber Café using a web camera installed on one of the computers in the Cyber Café for establishing the identity of the user. Such web camera photographs, duly authenticated by the user and authorised representative of cyber café, shall be part of the log register which may be maintained in physical or electronic form.

(4) A minor without photo Identity card shall be accompanied by an adult with any of the documents as required under sub-rule (1).

(5) A person accompanying a user shall be allowed to enter cyber café after he has established his identity by producing a document listed in sub-rule(1) and record of same shall be kept in accordance with sub-rule (2).

(6) The Cyber café shall immediately report to the concerned police, if they have reasonable doubt or suspicion regarding any user.

5. Log Register.— (1) After the identity of the user and any person accompanied with him has been established as per sub-rule (1) of rule 4, the Cyber Café shall record and maintain the required information of each user as well as accompanying person, if any, in the log register for a minimum period of one year.

(2) The Cyber Café may maintain an online version of the log register. Such online version of log register shall be authenticated by using digital or electronic

signature. The log register shall contain at least the following details of the user, namely : —

(i) Name
(ii) Address
(iii) Gender
(iv) Contact Number
(v) Type and detail of identification document
(vii) Date
(vii) Computer terminal identification
(viii) Log in Time
(ix) Log out Time

(3) Cyber Café shall prepare a monthly report of the log register showing date-wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by the 5th day of next month.

(4) The cyber café owner shall be responsible for storing and maintaining backups of following log records for each access or login by any user of its computer resource for at least one year:—

(i) History of websites accessed using computer resource at cyber café;
(ii) Logs of proxy server installed at cyber café.

Cyber Café may refer to "Guidelines for auditing and logging – CISG-2008-01" prepared and updated from time to time by Indian Computer Emergency Response Team (CERT-In) for any assistance related to logs. This document is available at www.cert-in.org.in

(5) Cyber café shall ensure that log register is not altered and maintained in a secure manner for a period of at least one year.

6. Management of Physical Layout and computer resource.— (1) Partitions of Cubicles built or installed if any, inside the Cyber Café, shall not exceed four and half feet in height from the floor level.

(2) The screen of all computers installed other than in Partitions or Cubicles, shall face 'outward', i.e. they shall face the common open space of the Cyber Café.

(3) Any Cyber Café having cubicles or partitions shall not allow minors to use any computer resource in cubicles or partitions except when they are accompanied by their guardians or parents.

(4) All time clocks of the computer systems and servers installed in the Cyber Café shall be synchronised with the Indian Standard Time.

(5) All the computers in the cyber café may be equipped with the commercially available safety or filtering software so as to the avoid as far as possible, access to the websites relating to pornography including child pornography or obscene information..

(6) Cyber Café shall take sufficient precautions to ensure that their computer resource are not utilised for any illegal activity.

(7) Cyber Café shall display a board, clearly visible to the users, prohibiting them from viewing pornographic sites as well as copying or downloading information which is prohibited under the law.

(8) Cyber Café shall incorporate reasonable preventive measures to disallow the user from tampering with the computer system settings.

(9) Cyber café shall maintain the user identity information and the log register in a secure manner.

(10) Cyber café shall also maintain a record of its staff for a period of one year.

(11) Cyber café shall not misuse or alter the information in the log register.

7. Inspection of Cyber Café : (1) An officer authorised by the registration agency, is authorised to check or inspect cyber café and the computer resource or network established therein at any time for the compliance of these rules. The cyber café owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

[F. No. 11(3)/2011-CLFE]
N. RAVI SHANKER, Jt. Secy.

अधिसूचना

नई दिल्ली, 11 अप्रैल, 2011

सा.का.नि. 316(अ).— केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 6क की उपधारा (2) के साथ पठित धारा 87 की उपधारा (2) के खंड (गक) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित, नियम बनाती है, अर्थात् :--

1. **संक्षिप्त नाम और प्रारंभ**- (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (इलेक्ट्रानिकी सेवा परिदान) नियम, 2011 है ।

(2) ये राजपत्र में इनके प्रकाशन की तारीख से प्रवृत्त होंगे ।

2. **परिभाषाएं** - इन नियमों में जब तक संदर्भ से अन्यथा अपेक्षित न हो,-

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "समुचित सरकार" से केन्द्रीय सरकार या राज्य सरकार या कोई संघ राज्यक्षेत्र अभिप्रेत है;

(ग) "प्राधिकृत अभिकर्ता" से समुचित सरकार का या सेवा प्रदाता का कोई अभिकर्ता अभिप्रेत है जिसके अंतर्गत किसी इलेक्ट्रानिकी समर्थ क्योस्क का प्रचालक भी है जिसे इन नियमों में विनिर्दिष्ट प्रक्रिया का अनुपालन करते हुए इन नियमों के अधीन उपयोक्ताओं को कंपयूटर संसाधनों या किसी संचार युक्ति की सहायता से लोक सेवा प्रदान करने के लिए अनुज्ञात किया गया है;

(घ) "प्रमाण पत्र" से इस अधिनियम, नियम, विनियम या समुचित सरकार के आदेश से सशक्त कानूनी प्राधिकारी द्वारा किसी व्यक्ति प्रकृत या कृत्रिम की प्रस्थिति, अधिकार या दायित्व की संपुष्टि करने के लिए जारी किया जाने वाला प्रमाण पत्र अभिप्रेत है जिसके अंतर्गत इलेक्ट्रानिकी रूप में मुद्रित और समुचित प्राधिकारी द्वारा यथाविनिर्दिष्ट ऐसे प्ररूप में परिदान प्रमाण पत्र भी है;

(ङ) "प्रमाणन प्राधिकारी" से अधिनियम की धारा 2 की उपधारा (1) के खंड (छ) में यथापरिभाषित प्रमाणन प्राधिकारी अभिप्रेत है;

(च) "संचार युक्ति" से अधिनियम की धारा 2 की उपधारा (1) के खंड (जक) में यथापरिभाषित संचार युक्ति अभिप्रेत है;

(छ) "कंप्यूटर संसाधन " से अधिनियम की धारा 2 की उपधारा (1) के खंड (ट) में यथापरिभाषित कंप्यूटर संसाधन अभिप्रेत है;

(ज) "इलेक्ट्रानिकी समर्थ क्योस्क" से अधिनियम की धारा 2 की उपधारा (1) के खंड (ढक) में यथापरिभाषित साइबर कैफे अभिप्रेत है;

(झ) "इलेक्ट्रानिकी सेवा परिदान " से प्ररूपों और आवेदनों की पावती दाखिल करना, किसी अनुज्ञप्ति, परमिट, प्रमाण पत्र, मंजूरी या अनुमोदन को जारी करना और नियम 3 के अधीन विनिर्दिष्ट प्रक्रिया का अनुपालन करते हुए इलेक्ट्रानिकी माध्यम द्वारा धन की प्राप्ति या संदाय अभिप्रेत है;

(ञ) "इलेक्ट्रानिकी हस्ताक्षर" से अधिनियम की धारा 2 की उपधारा (1) के खंड (नक) में यथापरिभाषित इलोक्ट्रॉनिकी हस्ताक्षर अभिप्रेत है;

(ट) " इलेक्ट्रानिकी हस्ताक्षर प्रमाणपत्र" से अधिनियम की धारा 2 की उपधारा (1) के खंड (नख) में यथापरिभाषित इलेक्ट्रॉनिकी हस्ताक्षर प्रमाणपत्र अभिप्रेत है;

(ठ) " इलेक्ट्रानिकी रूप में हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों का संग्रह " से इन नियमों के अनुसरण में इलेक्ट्रानिकी रूप में हस्ताक्षरित, भंडारित और प्रबंध किए जा रहे सभी अभिलेखों का संग्रह अभिप्रेत है;

(ड) "सेवा प्रदाता" से अधिनियम की धारा 6क की उपधारा (1) के स्पष्टीकरण में निर्दिष्ट सेवा प्रदाता अभिप्रेत है;

(ढ) "हस्ताक्षर करने वाला प्राधिकारी" से किसी अधिनियम, नियमों, विनियमों या प्रमाण पत्र जारी करने के लिए समुचित सरकार के आदेश के अधीन सशक्त कोई हस्ताक्षर करने वाला प्राधिकारी अभिप्रेत है;

३ इलेक्ट्रानिकी सेवा परिदान प्रणाली-

(1) समुचित सरकार स्वयं या अपने किसी प्राधिकृत अभिकरण के माध्यम से इलेक्ट्रानिकी रूप से समर्थ क्योस्क के या किसी अन्य इलेक्ट्रानिकी सेवा परिदान तंत्र के माध्यम से लोक सेवा प्रदान कर सकती है।

(2) समुचित सरकार या उसके अभिकरण इलेक्ट्रानिकी सेवा परिदान का प्ररूप और रीति विनिर्दिष्ट कर सकेंगे।

(3) समुचित सरकार गोपनीयता की अपेक्षा रखने वाले संवेदनशील इलेक्ट्रानिकी अभिलेखों को उनके इलेक्ट्रानिकी रुप में हस्ताक्षर करने के दौरान कूट करने की रीति विहित कर सकेगी।

(4) समुचित सरकार इलेक्ट्रानिकी सेवा परिदान के लिए प्राधिकृत सेवा प्रदाताओं और उनके अभिकर्ताओं को अधिसूचित करेगी।

(5) समुचित सरकार इलेक्ट्रॉनिकी सेवा परिदान प्रणाली को अंगीकार करके किए गए संदायों की पावती को ऐसी सरकार की वित्तीय संहिता और खजाना संहिता के अनुपालन में किए गए संदायों की

पावती अनुज्ञात कर सकती है।

(6) समुचित सरकार सेवा प्रदाताओं और उनके अभिकर्ताओं को उस व्यक्ति से जो ऐसी सेवा का उपयोग रहा है को ऐसी सेवा उपलब्ध कराने के प्रयोजन के लिए समुचित सरकार द्वारा यथाविनिर्दिष्ट ऐसे सेवा प्रभारों का संग्रहण करने के लिए, रखने के लिए और उपायोजित करने के लिए प्राधिकृत कर सकेगी।

परंतु यह कि उपायोजित सेवा प्रभारों को सेवा का उपयोग करने वाले व्यक्ति को दी जानी वाली पावती पर स्पष्ट रूप से उपदर्शित किया जाएगा।

(7) समुचित सरकार अधिसूचना द्वारा सेवा प्रदाताओं और उनके प्राधिकृत अभिकर्ताओं द्वारा प्रभारित और संग्रहित किए जाने वाले सेवा प्रभारों की दर को अधिसूचना द्वारा विनिर्दिष्ट करेगी।

(8) समुचित सरकार सेवा प्रदाताओं और उनके प्राधिकृत अभिकर्ताओं द्वारा सेवा स्तर के मानकों को भी विनिर्धारित कर सकेगी।

4. **इलेक्ट्रानिकी सेवा परिदान की अधिसूचना-**

(1) समुचित सरकार उन सेवाओं को अधिसूचित कर सकेगी जो समय-समय पर इलेक्ट्रानिकी रूप में परिदत्त की जानी हैं।

(2) समुचित सरकार समय-समय पर अनुज्ञप्तिधारियों, परमिटों, प्रमाणपत्रों, मंजूरियों, संदाय पावती अनुमोदनों के विभिन्न वर्गों के संबंध में उनकी संबंधित अधिकारिता की स्थानीय सीमाओं में हस्ताक्षर करने वाले प्राधिकारियों की सूची की पहचान और उसे अधिसूचित कर सकेगी।

(3) अधिसूचना प्रमाणपत्र की प्रकृति, समुचित सरकार द्वारा यथा अनुमोदित हस्ताक्षर करने वाले प्राधिकारियों के नाम, प्राधिकारिता के प्रभावी रहने की अवधि और उनकी अधिकारिता की सीमा को विनिर्दिष्ट करेगी।

(4) समुचित सरकार समय-समय पर हस्ताक्षर करने वाले प्राधिकारियों की सूची में हस्ताक्षर करने वाले प्राधिकारी की हैसियत रखने वाले कर्मचारियों की सेवा के निबंधन और शर्तों पर विचार करते हुए परिवर्तनों को अधिसूचित कर सकेगी।

5. **इलेक्ट्रानिकी रूप में हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों के संग्रह का सरकारी प्राधिकारियों द्वारा सृजन-**

(1) सभी प्राधिकारी जो इलेक्ट्रानिक माध्यम से कोई अनुज्ञप्ति, परमिट, प्रमाणपत्र, स्वीकृति या अनुमोदन जारी करते हैं यथास्थिति इलेक्ट्रानिकी रूप में हस्ताक्षरित ऐसी अनुज्ञप्तियों, परमिटों, प्रमाणपत्रों, स्वीकृतियों या अनुमोदनों के इन व्यष्टिक अभिलेखों के सृजन के समय को दर्शित करते हुए उनका एक आन लाइन संग्रह तैयार करेंगे, अभिलेखागार बनाएंगे और उसका अनुरक्षण करेंगे।

(2) समुचित सरकार उपनियम (1) में निर्दिष्ट इलेक्ट्रानिकी रूप में हस्ताक्षरित संग्रह तैयार करने, प्रतिष्ठापित करने, अभिलेखागार बनाने और उसका अनुरक्षण करने की रीति विनिर्दिष्ट कर सकेगी।

(3) प्राधिकारी इलेक्ट्रानिकी रूप में ऐसी अनुज्ञप्तियों, परमिटों, प्रमाणपत्रों, स्वीकृतियों या अनुमोदनों के प्रत्येक अभिलेख पर या समग्र पर विनिर्दिष्ट अवधि के लिए हस्ताक्षर कर सकेंगे और उनका आन लाइन

प्रशासन करने के लिए उत्तरदायी होंगे।

(4) समुचित सरकार इलेक्ट्रानिकी डाटा, सूचना, आवेदन, डिजिटल रूप से हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों और उनके क्रमशः नियंत्रण में सूचना प्रौद्योगिकी आस्तियों के लिए सुरक्षा प्रक्रिया विनिर्दिष्ट कर सकेगी और सुरक्षा प्रक्रिया का अनुपालन विभागाध्यक्ष और हस्ताक्षर करने वाले प्राधिकारियों द्वारा किया जाएगा।

स्पष्टीकरण- उपनियम (1) में निर्दिष्ट सुरक्षा प्रक्रिया में गूढ़ालेखी कुंजियों के भंडारण और अनुरक्षण की अपेक्षाओं, ब्राउज़रों पर प्रमाणपत्र डाउनलोड करने पर निर्बंधन और प्रमाणन प्राधिकारियों की अपेक्षाओं का अनुपालन करना भी है।

6. इलेक्ट्रानिक रूप से हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों के संग्रह में परिवर्तन करने की प्रक्रिया

(1) समुचित सरकार या स्वप्रेरणा से या किसी हितबद्ध पक्षकार से आवेदन अभिप्राप्त होने पर इलेक्ट्रानिक रूप से हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों के संग्रह में परिवर्तन करने के कारणों को अभिलिखित करते हुए समुचित परिवर्तन कर सकेगी या करने का आदेश कर सकेगी।

(2) इलेक्ट्रानिक रूप से हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों के किसी संग्रह के किसी अभिलेख में किया गया कोई परिवर्तन और ऐसे संग्रह से किसी अभिलेख का वर्धन या लोप उस व्यक्ति द्वारा मूल सृजन के समय और उपांतरणों के समय की मोहर के साथ जो ऐसा परिवर्तन करने के लिए सक्षम है, इलेक्ट्रानिक रूप से हस्ताक्षरित किया जाएगा।

(3) समुचित सरकार इलेक्ट्रानिक रूप से हस्ताक्षरित इलेक्ट्रानिकी अभिलेखों के संग्रह से किसी अभिलेख का लोप करने की घटना को इलेक्ट्रानिक रूप से हस्ताक्षर करने की रीति को विहित कर सकेगी।

(4) समुचित सरकार डिजिटल रूप से हस्ताक्षरित अभिलेखों के संग्रह के सुरक्षित एक्सेस की रीति के उपबंध को भी विनिर्धारित कर सकेगी।

(5) समुचित सरकार डिजिटल रूप से हस्ताक्षरित इलेक्ट्रानिक अभिलेखों के संग्रह का अनुरक्षण करने के लिए प्रभारों की लेखा परीक्षा की अपेक्षाओं को भी विनिर्धारित कर सकेगी।

7. सेवा प्रदाता और प्राधिकृत अभिकर्ता का वितीय प्रबंधन और लेखांकन का दायित्व

समुचित सरकार प्रत्येक सेवा प्रदाता और प्राधिकृत अभिकर्ता को सभी संव्यवहारों, पावतियों, वाउचरों का अद्यतन और शुध्द लेखा रखने के लिए तथा परिदत्त इलेक्ट्रानिकी सेवा के संबंध में संव्यवहारों और संदाय की पावतियों के लेखे का अनुरक्षण करने के लिए प्ररूप विनिर्दिष्ट करने के लिए निदेश दे सकेगी और उक्त अभिलेखों को निरीक्षण और लेखा परीक्षा के लिए समुचित सरकार द्वारा नामनिर्दिष्ट किसी अभिकरण या व्यक्ति के समक्ष प्रस्तुत किया जाएगा।

8. सेवा प्रदाता और प्राधिकृत अभिकर्ताओं की सूचना प्रणाली और खातों की लेखा परीक्षा

(1) समुचित सरकार राज्य में सेवा प्रदाता और प्राधिकृत अभिकर्ताओं के कार्यकलापों की ऐसे अंतरालों पर, जो वह उचित समझे, नामनिर्दिष्ट लेखा परीक्षा अभिकरणों द्वारा लेखा परीक्षा का संचालन कारित करेगी।

(2) लेखा परीक्षा में सुरक्षा , गोपनीयता और सूचना की एकांतता और इलेक्ट्रानिकी सेवा परिदान में किसी सॉफ्टवेयर के अनुप्रयोग का कार्य निष्पादन और सेवा प्रदाता और प्राधिकृत अभिकर्ताओं द्वारा रखे गए लेखों की शुध्दता जैसे पहलू होंगे।

(3) आडिट अभिकरणों द्वारा दिए गए निदेशों का अनुपालन करने के लिए और लेखा परीक्षा अभिकरणों द्वारा इंगित त्रुटियों को दूर करने के लिए लेखा परीक्षा अभिकरणों द्वारा विनिर्दिष्ट समयसीमा के भीतर सेवा प्रदाता और प्राधिकृत अभिकर्ता समुचित प्राधिकारी द्वारा नामनिर्दिष्ट लेखा परीक्षा अभिकरणो को सूचना और सहायता उपलब्ध कराएंगे।

(4) सभी सेवा प्रदाता और प्राधिकृत अभिकर्ता प्रत्येक व्यष्टिक अंतरण और नागरिक के डाटा के संरक्षण के लिए सम्यक घोषणा प्रस्तुत करेंगे और व्यष्टिक या समुचित संरकार में से किसी एक की लिखित सहमति के बिना किसी को आप्राधिकृत प्रकटन ऐसे सेवाप्रदाता को आगे ऐसी और सेवा प्रदान करने से रोक देगा और ऐसे मामलों में अधिनियम की धारा 45 के उपबंध लागू होंगे।

9. **इलेक्ट्रानिकी सेवा परिदान में विशेष लेखन सामग्री का उपयोग** - समुचित सरकार इलेक्ट्रानिकी सेवा परिदान के भाग के रूप में प्ररूपों, आवेदन, अनुज्ञप्ति,परमिट, प्रमाण पत्र, भुगतान की पावती तथा ऐसे अन्य दस्तावेजों के लिए सुरक्षा अभिलक्ष णों से युक्त विभिन्न प्रकार की विशेष लेखन सामग्री विनिर्दिष्ट कर सकेगी।

[फा. सं. 11(3)/2011-सीएलएफई]

शंकर अग्रवाल, अपर सचिव

NOTIFICATION

New Delhi, the 11th April, 2011

G.S.R. 316(E).—In exercise of the powers conferred by clause (ca) of sub-section (2) of section 87, read with sub-section (2) of section 6A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:-

1. **Short title and commencement.**- (1) These rules may be called the Information Technology (Electronic Service Delivery) Rules, 2011.
   (2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions.**- In these rules, unless the context otherwise requires,-
   (a) "**Act**" means the Information Technology Act, 2000 (21 of 2000);

(b) **"appropriate Government"** means the Central Government or the State Government or an Union Territory Administration;

(c) **"authorised agent"** means an agent of the appropriate Government or service provider and includes an operator of an electronically enabled kiosk who is permitted under these rules to deliver public services to the users with the help of a computer resource or any communication device, by following the procedure specified in the rules;

(d) **"certificate"** means a certificate required to be issued by a statutory authority empowered under any Act, rule, regulation or Order of the appropriate Government to issue a certificate to confirm the status, right or responsibility of a person, either natural or artificial, and includes a certificate in electronic form printed and delivered in such form as may be specified by the appropriate authority;

(e) **"Certifying Authority"** means certifying authority as defined in clause (g) of sub-section (1) of section 2 of the Act;

(f) "**communication device**" means the communication device as defined in clause (ha) of sub-section (1) of section 2 of the Act;

(g) **"computer resource"** means the computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(h) "**Electronically enabled kiosk"** means the cyber cafe as defined in clause (na) of sub-section (1) of section 2 of the Act;

(i) "**Electronic Service Delivery"** means the delivery of public services in the form of filing receipt of forms and applications, issue or grant of any license, permit, certificate, sanction or approval and the receipt or payment of money by electronic means by following the procedure specified under rule 3;

(j) "**electronic signature**" means the electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

(k) "**Electronic Signature Certificate**" means the electronic signature certificate as defined in clause (tb) of sub-section (1) of section 2 of the Act;

(l) "**Repository of Electronically Signed Electronic Records**" means a collection of all electronically signed electronic records, stored and managed in accordance with these rules;

(m)"**service provider**" means a service provider as referred to in Explanation to sub-section (1) of section 6A of the Act;

(n) "**signing authority** " means an authority empowered under any Act, rules, regulations or Order of the appropriate Government to issue a certificate.

3. System of Electronic Service Delivery.-

(1) The appropriate Government may on its own or through an agency authorised by it, deliver public services through electronically enabled kiosks or any other electronic service delivery mechanism.

(2) The appropriate Government or its agencies may specify the form and the manner of Electronic Service Delivery.

(3) The appropriate Government may determine the manner of encrypting sensitive electronic records requiring confidentiality, while they are electronically signed.

(4) The appropriate Government shall notify the service providers and their agents authorised for Electronic Service Delivery.

(5) The appropriate Government may allow receipt of payments made by adopting the Electronic Service Delivery System to be a deemed receipt of payment effected in compliance with the financial code and treasury code of such Government.

(6) The appropriate Government may authorise service providers or their authorised agents to collect, retain and appropriate such service charges as may be specified by the appropriate Government for the purpose of providing such services from the person availing such services:

Provided that the apportioned service charges shall be clearly indicated on the receipt to be given to the person availing the services.

(7) The appropriate Government shall by notification specify the scale of service charges which may be charged and collected by the service providers and their authorised agents for various kinds of services.

(8) The appropriate Government may also determine the norms on service levels to be complied with by the Service Provider and the authorised agents.

4. Notification of Electronic Service Delivery.-

(1) The appropriate Government may notify the services that shall be delivered electronically from time to time.

(2) The appropriate Government may identify and notify, from time to time, the list or signing authorities in respect of different classes of licenses, permits, certificates, sanctions, payment receipt approvals and local limits of their respective jurisdictions.

(3) The notification shall specify the nature of certificate, the names of the signing authorities, as approved by the appropriate Government, the period of effectiveness of the authority and the extent of their jurisdiction.

(4) The appropriate Government may notify changes to the list of signing authorities from time to time, taking into consideration the terms and conditions of the services of employees holding positions of signing authorities.

5. Creation of repository of electronically signed electronic records by Government Authorities.-

(1) All authorities that issue any license, permit, certificate, sanction or approval electronically, shall create, archive and maintain a repository of electronically signed electronic records of such licenses, permits, certificates, sanctions or approvals, as the case may be, online with due timestamps of creation of these individual electronic records.

(2) The appropriate Government may specify the manner of creating, establishing, archiving and maintaining the repository of electronically signed electronic records referred to in sub-rule (1).

(3) The authorities may electronically sign the electronic records of such licenses, permits, certificates, sanctions or approvals for each record or as a whole for a specific duration and shall be responsible in administering them online.

(4) The appropriate Government may specify the security procedures in respect of the electronic data, information, applications, repository of digitally signed electronic records and information technology assets under their respective control and that security procedures shall be followed by the Head of the Department and the signing authorities.

Explanation.- The expression "security procedures" referred to in sub-rule (4) shall include requirements for the storage and management of

cryptographic keys, restrictions for downloading the certificates on to browsers, and of complying with the requirements of certifying authorities.

6. **Procedure for making changes in a repository of electronically signed electronic records.-**

(1) The appropriate Government may either suo moto or after receiving an application from an interested party, make or order to make an appropriate change in a repository of electronically signed electronic records along with recording the reasons for making such a change.

(2) Any change effected to any record in a repository of electronically signed electronic records and any addition or deletion of a record from such repository shall be electronically signed by the person who is authorised to make such changes along with the time stamps of original creation and modification times.

(3) The appropriate Government may determine the manner of electronically signing the event of deletion of a record from the repository of electronically signed electronic records.

(4) The appropriate Government may also determine the manner of provisioning secure access to the repository of digitally signed electronic records.

(5) The appropriate Government may also determine the requirements for maintaining audit trails of all changes made to repository of digitally signed electronic records.

7. **Responsibility of service provider and authorised agents for financial management and accounting.-** The appropriate Government may direct every service provider and authorised agent to keep an updated and accurate account of the transactions, receipts, vouchers and specify the formats for maintaining accounts of transactions and receipt of payment in respect of the electronic services delivered and the said records shall be produced for inspection and audit before an agency or person nominated by the appropriate Government.

8. **Audit of the Information System and Accounts of service provider and authorised agents.-**

(1) The appropriate Government may cause an audit to be conducted of the affairs of the service providers and authorised agents in the State at such intervals as deemed necessary by nominating such audit agencies.

(2) The audit may cover aspects such as the security, confidentiality and the privacy of information, the functionality and performance of any software application used in the electronic service delivery and the accuracy of accounts kept by the service providers and authorised agents.

(3) The service providers and the authorised agents shall provide such information and assistance to the audit agencies nominated by the appropriate authority, to comply with the directions given by the audit agencies and to rectify the defects and deficiencies pointed out by the audit agencies within the time limit specified by the audit agency.

(4) All service providers and the authorised agents shall submit a due declaration for protecting the data of every individual transaction and citizen and any unauthorised disclosure to anyone without the written consent of either the individual or the appropriate Government shall be debarred from providing such a service any further and the provisions of section 45 of the Act shall be applicable in such cases.

9. **Use of special stationery in electronic service delivery.-** The appropriate Government may specify different types of special stationery, with accompanying security features for forms, applications, licenses, permits, certificates, receipts of payment and such other documents as part of Electronic Service Delivery.

[F. No. 11(3)/2011-CLFE]
SHANKAR AGGARWAL, Addl. Secy.

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.